COE 4.x Security Update

Mr. Matt O'Brien
SAIC
(703) 676-5032
obrienma@saic.com

Mr. Quang Nguyen
COE Security Engineer
Defense Information Systems Agency
(703) 882-1119
nguye2q@ncr.disa.mil

Agenda

- **Lockdown Status**
- **IAVA Segmented Patch Release Issue**
- **Security Tools Status**
- **Plans**
- **Background Briefings**
  - **Lockdown Status**
  - **W2KCET 4.5.1.0 Security Lockdown Templates**
  - **IAVA Patch Release Process**
  - **Segment Security Compliance**

Lockdown Status

- **Windows Security Lockdown Status**
  - **Security lockdown templates for Win2K (W2KCET 4.5.1.0) to be delivered end of Jan ’02**
  - **This delivery will complete 2-step lockdown process (kernel + templates) for all 3 Win2K OSs**
- **UNIX Security Lockdown Status**
  - **Security Policy Configuration Tool (SPCFG 4.2.0.0) will use two security templates**
    - **SPCFGD 4.2.0.5 template re-applies kernel security lockdown**
    - **SPVULD will provide security vulnerability fixes not addressed by patch segments (e.g., configuration changes)**
      - ✓ **Delivery 1st Qtr ‘02**
  - **SPCFG port to HP-UX 11.0 to be completed 1st Qtr ‘02**

Lockdown Issues

- **Windows Security Lockdown**
  - **W2KCET 4.5.1.0 contains a number of security enhancements that modify the registry and delete files**
    - **These changes are based upon NSA guidance**
      - ✓ **Example: Modify registry to disable access by Novell clients**
      - ✓ **Example: Deletion of POSIX and OS2 subsystems**
  - **These changes are documented in W2KCET 4.5.1.0 brief and should be evaluated for compatibility with systems' CONOPS**
    - **See Notes Pages of W2KCET 4.5.1.0 briefing for rationale**
  - **These changes are made based upon NSA guidance**
- **UNIX Security Lockdown**
  - **Need for a second security lockdown template**
    - **Provide vulnerability fixes throughout operational lifecycle**
      - ✓ **SPVULD will enable enhancements to security configuration baseline through configuration changes (e.g., changing a file's permissions)**
      - ✓ **Patch segments will continue to play their usual role**

IAVA Segmented Patch Release Issue

- **Questions about timeliness of COE's segmented IAVA patch release process**
  - **Patch is not available within 30-day compliance window**
    - **Reasons:**
      - ✓ **Complexity of OS patch segment integration testing requirements**
      - ✓ **Documentation requirements**
      - ✓ **LOE/available resources**
    - **Un-segmented patches made available to COE-based systems to facilitate meeting compliance deadline**
  - **COE Engineering Office evaluating requirements to support 30-day fielding of patch segments**

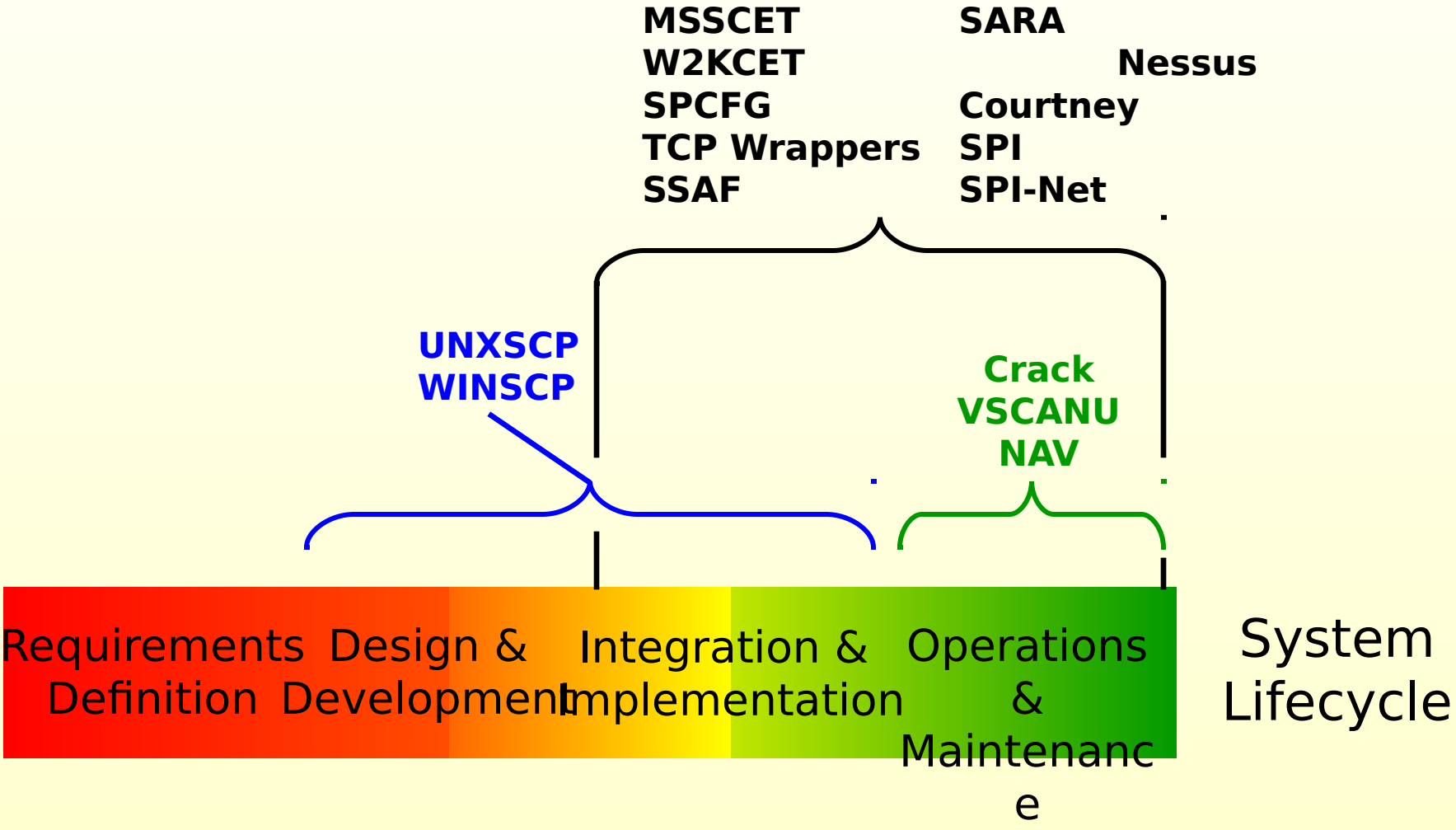
Security Tools Update

- **COE Security team provides a suite of (GOTS and COTS) security tools to be used during the security engineering lifecycle**
- **These tools are categorized by function and the lifecycle phase(s) in which they are used**

Security Tools By Function

- **Segment Security Compliance**
  UNXSCP WINSCP
- **Security Configuration Baseline (“Lockdown”)**
  MSSCET W2KCET SPCFG SPCFGD, SPVULD
- **Host/Network Security Configuration**
  TCP Wrappers SSAF (MSSCET, W2KCET & SPCFG)
- **Vulnerability Assessment and Monitoring**
  Crack SARA Nessus Courtney SPI SPI-Net
- **Anti-virus**
  VSCANU NAV

Security Tools in the System Lifecycle



Security Tools: Something Old, Something New

- **COTS security tools evolve just like other technologies**
  - **Something old (deprecated):**
    - **SATAN (superseded by SARA)**
    - **TRIPWIRE (licensing issues)**
  - **Something new (new segments):**
    - **SARA (successor to SATAN)**
    - **Courtney (detects SATAN/SARA scans)**
    - **Nessus (delivery soon)**
- **COE Security team periodically evaluates COTS security tools**

Security Tools: Description & Availability

Security Tool	Segment Prefix	Version #	Solaris 7	Solaris 8	HP-UX 11.0	Win NT 4.0	Win2K	Description
Crack	CRACK	4.0.0.1	X	?				Password-cracking utility
Crack	CRACK	1.0.0.4			?			Password-cracking utility
Courtney	CRTNEY	4.5.0.0	X	X				Detects port scans by SATAN and SARA
NT Security Lockdown Templates	MSSCET	4.5.0.0				X		Defines COE security configuration baseline using Microsoft templates; templates can be configured to be system-specific
Norton Anti-virus	NAV	4.5.1.0				X	X	Detects viruses and malicious code
Nessus Security Scanner	NESSUS	4.5.0.0/1.0.9	X	X	X			Scans networks for security vulnerabilities
SARA	SARA	4.5.0.0/3.4.9A	X	X	X			Scans networks for security vulnerabilities
Security Policy Configuration Tool	SPCFG	4.2.0.0	X	X				Defines COE security configuration baseline using GOTS templates; templates can be configured to be system-specific
Security Profile Inspector (SPI)	SPI	4.0.0.0/2.10				X	X	Vulnerability and intrusion detection tool
SPI-Net	SPINET	4.3.0.0/1.10			X			Vulnerability and intrusion detection tool
SPI-Net	SPINET	4.0.0.0/1.10	X					Vulnerability and intrusion detection tool
SPI-Net	SPINET	4.4.0.0/1.10		X				Vulnerability and intrusion detection tool

Key	X	Segmented and tested
	?	Segmented, but not tested for OS

Security Tools: Description & Availability

Security Tool	Segment Prefix	Version #	Solaris 7	Solaris 8	HP-UX 11.0	Win NT 4.0	Win2K	Description
SSAF	COESS NSSLIB	4.4.0.0/4.4.0.1 4.4.0.0/4.4.0.1	X	X	X	X	X	Provides client-server communications security using SSL and DoD PKI certificates
TCP Wrappers	TCPW	4.0.0.0	X	?				Used to monitor and filter connections to network services
TCP Wrappers	TCPW	4.3.0.0			X			Used to monitor and filter connections to network services
UNIX Security Compliance Process	N/A	1.2.0.0	X	X	X			Segment security compliance tool
VirusScan for UNIX	VSCANU	4.0.0.0/4.7	X	?				Detects viruses and malicious code
VirusScan for UNIX	VSCANU	4.3.0.0/4.12.0			X			Detects viruses and malicious code
Windows Security Compliance Process	N/A	1.2.0.0				X	X	Segment security compliance tool
Win2K Security Lockdown Templates	W2KCET	4.5.0.0					X	Defines COE security configuration baseline using Microsoft templates; templates can be configured to be system-specific

Key	X	Segmented and tested
	?	Segmented, but not tested for OS

Plans

- **Security team will complete suite of GOTS security tools and templates for security configuration baseline ("lockdown") in 1st Qtr '02**
- **Primary focus will shift to maintenance and enhancement of tools, templates & processes**
  - **Tiger Team Input**
  - **SEWG Input for C² lockdown templates**

Background Briefings

COE 4.x
Security Lockdown Status

11 January 2002

Agenda

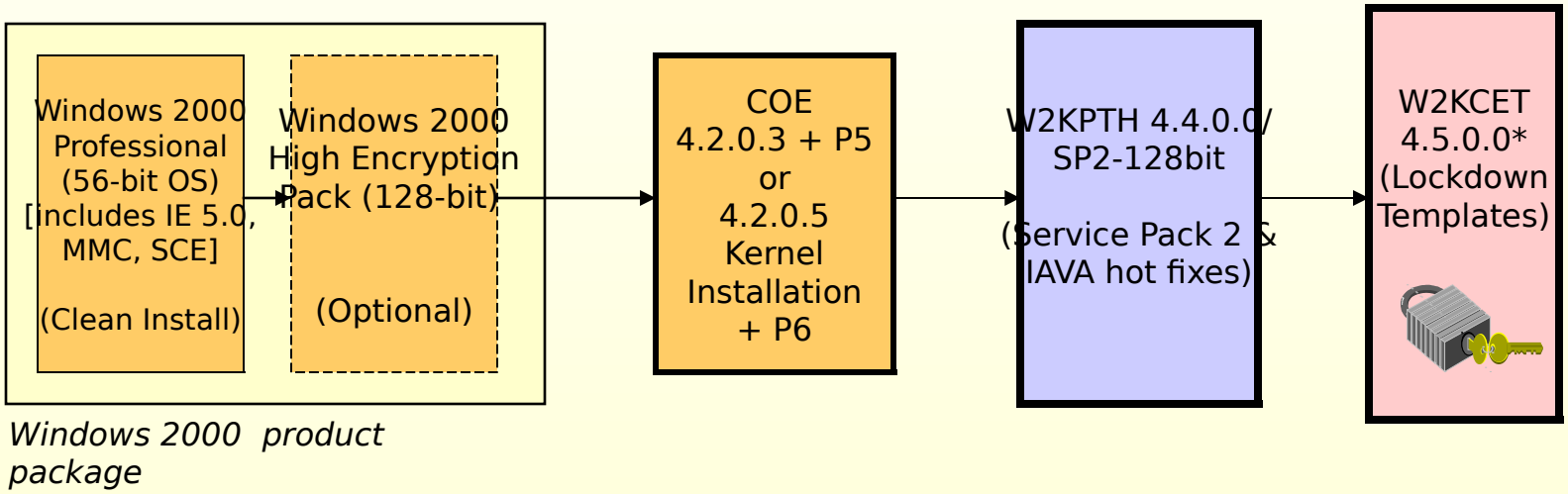
- **Lockdown Status**
- **Win2K Lockdown**
- **NT Lockdown**
- **Solaris Lockdown**

Lockdown Status

- **Windows Security Lockdown Status**
  - **Security lockdown templates for Win2K (W2KCET 4.5.1.0) to be delivered end of Jan ’02**
  - **This delivery will complete 2-step lockdown process (kernel + templates) for all 3 Win2K OSs**
- **UNIX Security Lockdown Status**
  - **Security Policy Configuration Tool (SPCFG 4.2.0.0) will use two security templates**
    - **SPCFGD 4.2.0.5 template re-applies kernel security lockdown**
    - **SPVULD will provide security vulnerability fixes not addressed by patch segments (e.g., configuration changes)**
      - ✓ **Delivery 1st Qtr ‘02**
  - **SPCFG port to HP-UX 11.0 to be completed 1st Qtr ‘02**

Win2K Security Lockdown

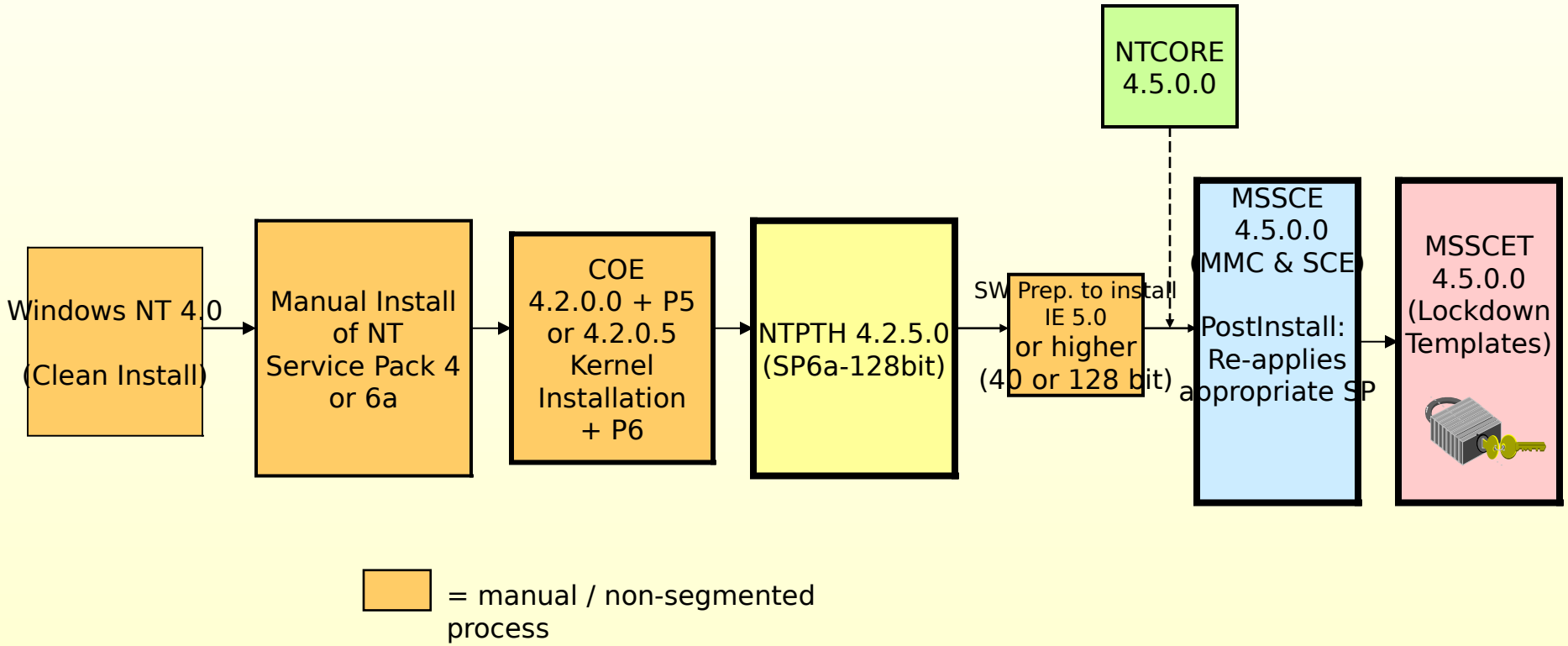
Win2K Installation Sequence for 4.2.0.0P6



* W2KCET 4.5.1.0 will provide support for Member Servers and Domain Controllers; end of January '02 delivery is expected.

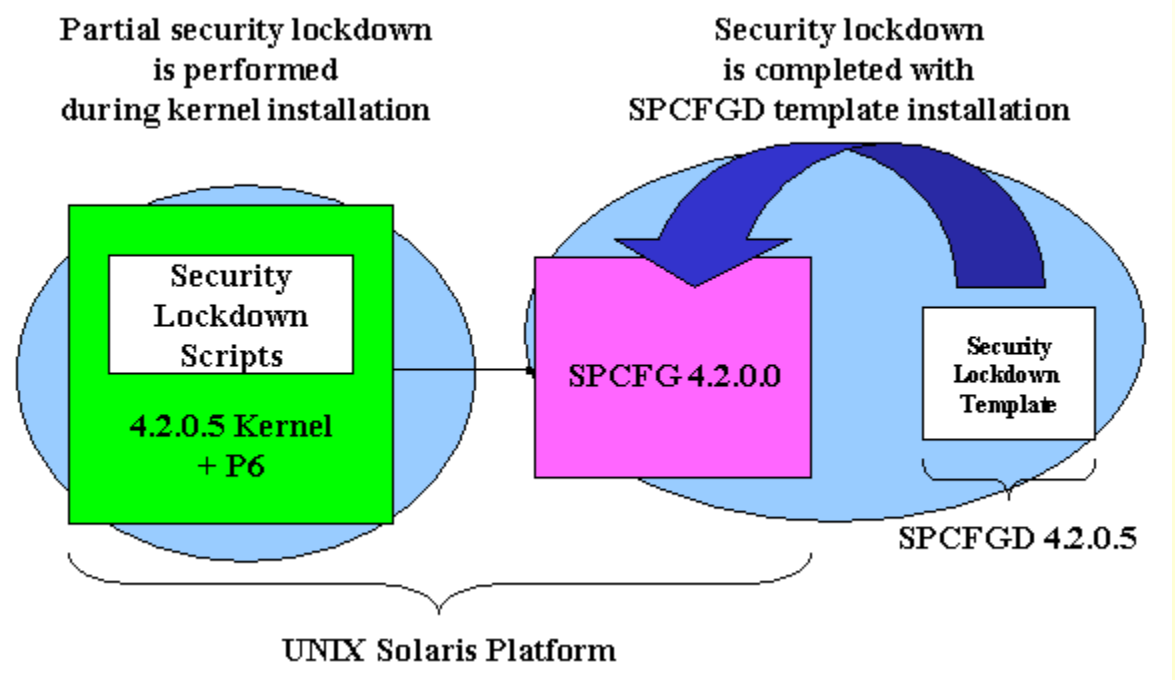
NT Security Lockdown

NT Installation Sequence for 4.2.0.0P6



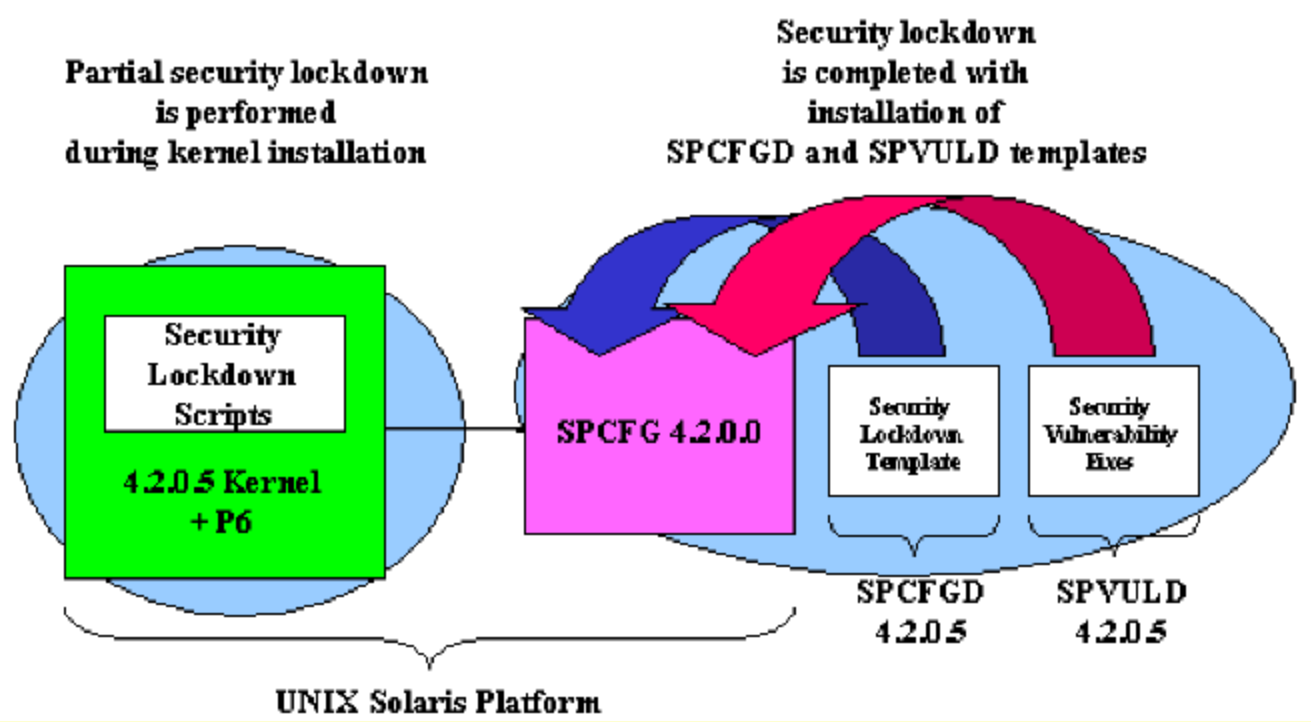
Solaris Security Lockdown

- **The Solaris security lockdown is currently a 2-step process**
- **SPCFG 4.2.0.0 is used to re-apply the security lockdown with the SPCFGD 4.2.0.5 secu**



Solaris Security Lockdown (2)

- **The Solaris security lockdown will become a 3-step process**
- **SPCFG will be used to apply the SPVULD security lockdown template for JAVA and oth**



W2KCET 4.5.1.0
Windows 2000
Security Lockdown Templates

11 January 2002

Agenda

- **Overview**
- **W2KCET 4.5.1.0 Enhancements**
- **Delivery Schedule**

Overview

- **W2KCET 4.5.1.0 will provide support for Windows 2000 Member Server and Domain Controller operating systems in addition to Professional**
- **The security lockdown templates in W2KCET 4.5.1.0 also contain enhancements that were not included in W2KCET 4.5.0.0 (Professional only)**
- **A beta version of W2KCET 4.5.1.0 has been made available to the COE community for feedback**

W2KCET 4.5.1.0 Enhancements

- **The segment includes the Microsoft Windows 2000 Resource Kit tool Kixtart (by permission) to run *.bat files included in the segment**
  - **These are used for dialog boxes during installation**
- **A number of registry keys are modified per NSA guidance**
- **A number of files are deleted per NSA guidance**

Registry Keys Modifications

- **The Novell FPNW registry entry has been removed from the Notification Package registry entry**
- **A registry entry to disable "automatically update the machine policy" has been added**
- **Instructions are provided for importing a machine policy, and a script is provided to re-enable the machine policy update feature**

Registry Key Modifications (2)

- **A registry entry has been added to prevent automatic administrator logon**
- **A registry entry has been added to prevent guest users from accessing event logs**
- **A registry entry has been added to prevent guest users from accessing the registry**
- **A registry entry has been added to prevent the auto run feature on any drive on the system (this includes floppies, network, or any other installed drive)**

Registry Key Modifications (3)

- **A registry entry has been added to prevent users from changing or replacing DLLs**
- **A registry entry has been added to prevent LM hash entries**

File Deletions

- **All OS2 and POSIX files will be removed from the system**
- **The OS2 directory will also be deleted**

Delivery Schedule

- **W2KCET 4.5.1.0 was released as a beta segment on 14 December 2001**
- **Delivery of the segment to DISA is currently scheduled for January 2002**

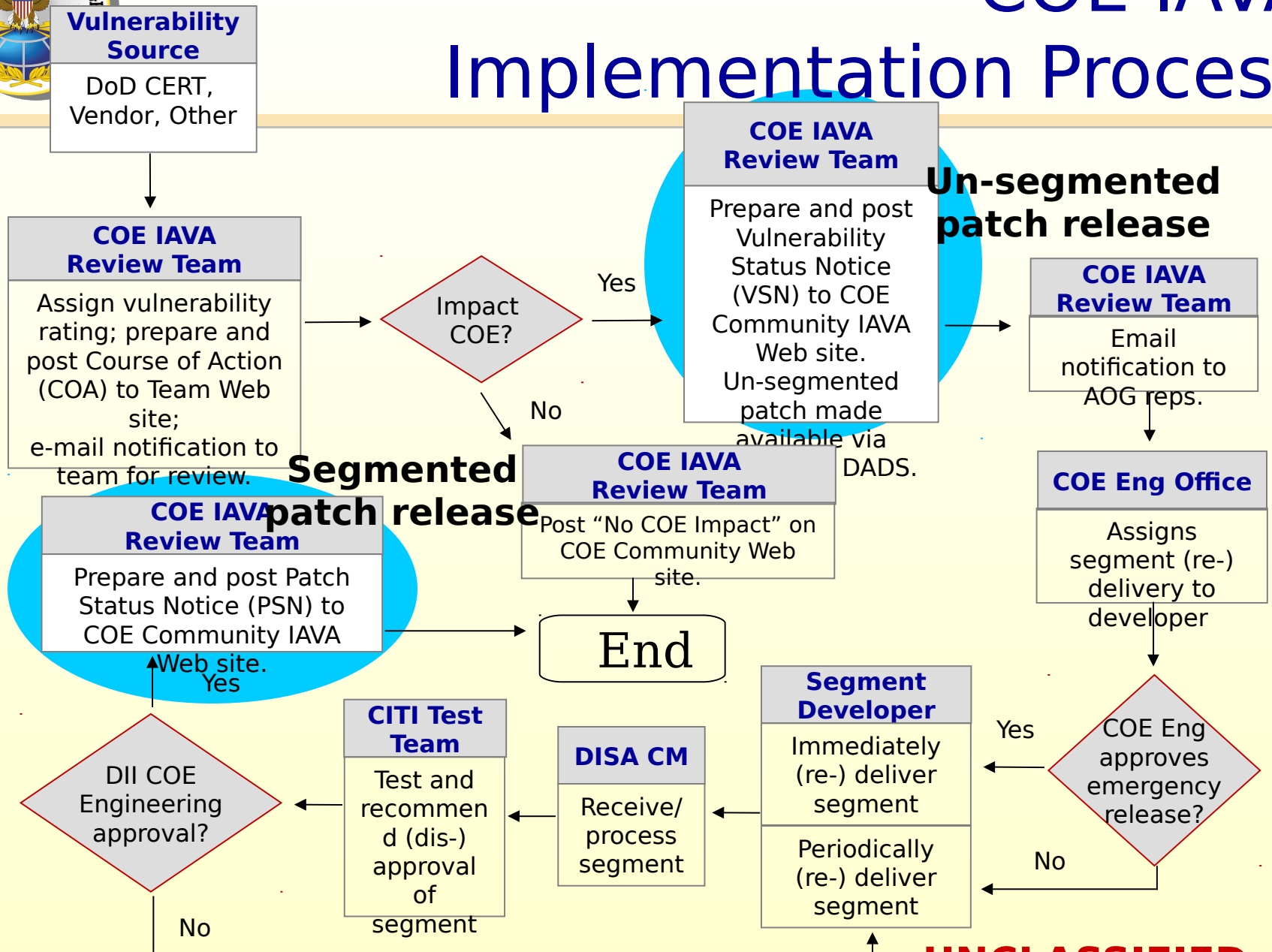
COE 4.x
IAVA Patch Release Process

11 January 2002

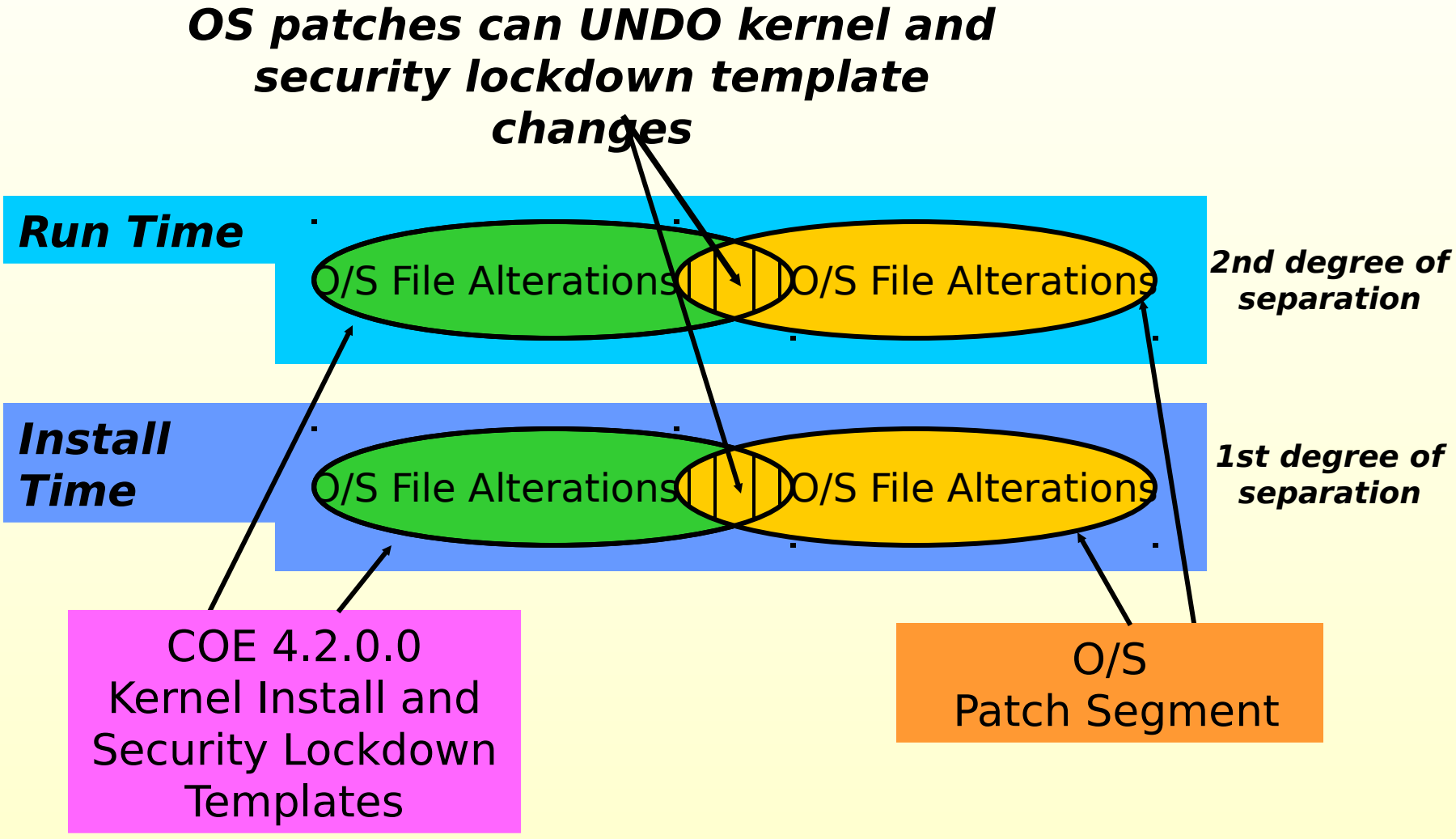
COE IAVA Patch Release Process

- **Patches are released in two ways:**
  - **Un-segmented patch via IAVA Web site and DADS**
    - **Correct patch is available quickly from trusted sites**
    - **Integration testing is responsibility of COE-based system**
  - **Segmented patch is incorporated into patch segment or appropriate application segment**
    - **Release schedule determined by COE Chief Engineer (triage function)**
    - **Integration testing is performed by COE Engineering Office**
- **Long-standing policy**
  - **Formally presented to AOG (4/01) and CRCB (5/01)**

COE IAVA Implementation Process



OS Patch Segment Integration Testing



COE 4.x
Segment Security Compliance

11 January 2002

Segment Security Compliance Requirements

- **Segments must be able to operate with kernel and template security lockdown**
- **Segment developer security requirements are contained in the *4.1 Integration and Runtime Specification***
  - **Chapter 4 (Security)**
  - **Appendix B (Security compliance items at Levels 2, 4-8)**
- **Security requirements emphasize:**
  - **File and directory permissions (Chap 4 Tables 4-1 & 4-2)**
  - **Best security practices (detailed in Chapter 4 and Appendix B)**

Segment Security Compliance Requirements (2)

- **Compliance is validated using segment security compliance tools**
  - **Developer environment**
  - **DISA acceptance testing**
- **ValidateSegSecurity output report must be included with segment**
- **Waiver requests must be submitted with justification**

Segment Security Compliance Tools

- **Tools for both Windows and UNIX segments are now available**

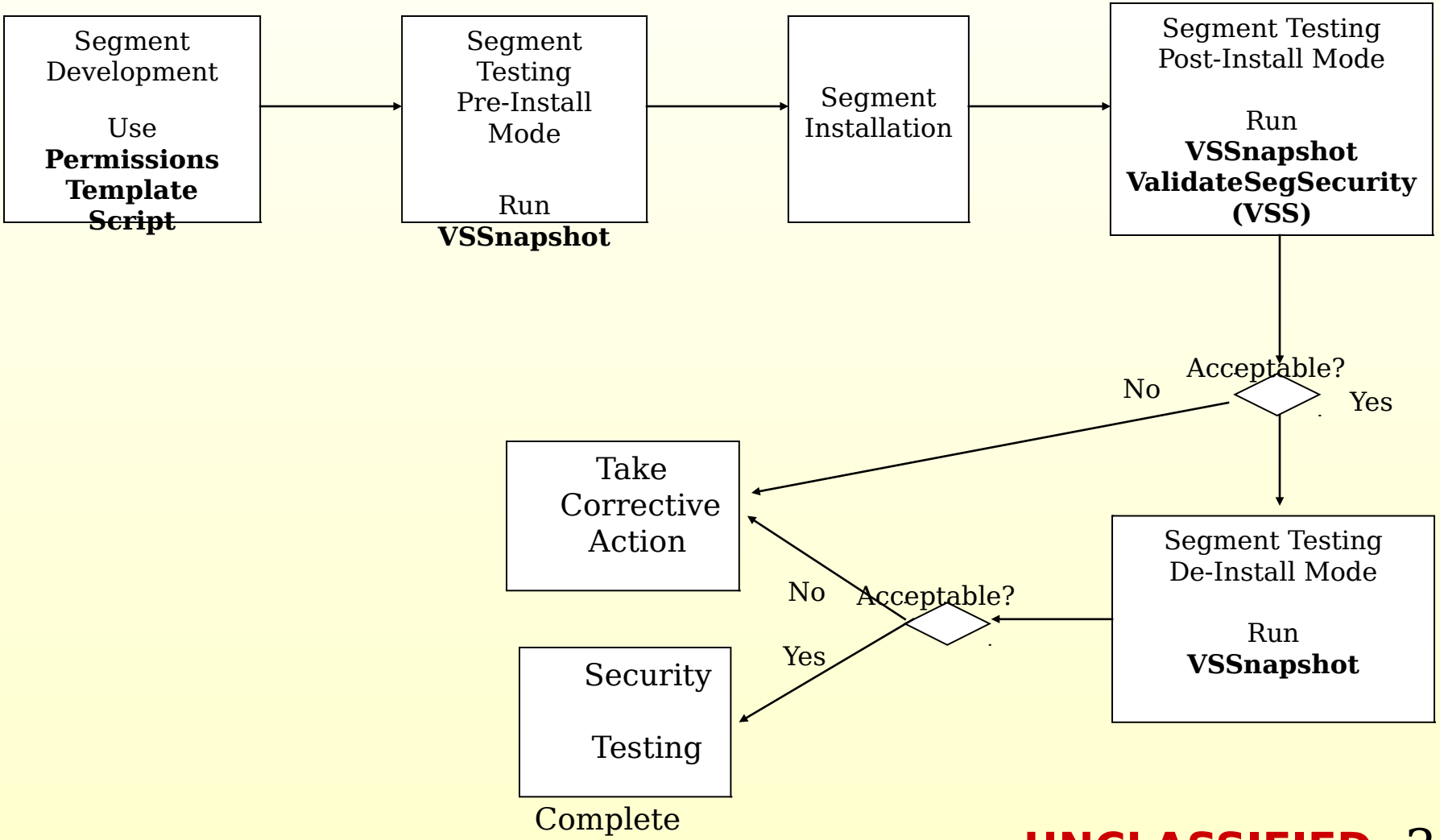
- **Windows Security Compliance Process (WINSCP) for Win2K and NT segments**
  - **Software: CM # 50109**
  - **User's Manual: CM # 50111 (soon superseded by # 52662)**

- **UNIX Security Compliance Process (UNXSCP) for Solaris 7/8 and HP-UX 11.0 segments**

WINSCP Overview

- **WINSCP provides three principal capabilities:**
  - **Windows complement to UNIX FileAttribs capability to enable segment developers to set directory and file permissions using a template batch script**
  - **Windows segment security compliance using ValidateSegSecurity (VSS) script**
  - **System “snapshot” capability using VSSnapshot script**

WINSCP Process



UNXSCP Overview

- **UNXSCP provides two principal capabilities:**
  - **UNIX (Sol 7&8, HP-UX 11.0) segment security compliance using ValidateSegSecurity (VSS) script**
  - **System "snapshot" capability using VSSnapshot script**
- **UNXSCP supersedes ValidateSegSecurity 1.1**

UNXSCP Process